Les questions juridiques particulières posées en Belgique par le projet du serveur S3

Verhaegen, Marie-Noelle; Herveg, Jean

Published in:
Réseaux de soins, de santé et réseaux de recherche médicale, Aspects légaux et responsabilités, Bilan des expériences

Publication date:
2003

Document Version
le PDF de l'éditeur

SÉLECTION DE QUESTIONS JURIDIQUES PARTICULIÈRES POSÉES EN BELGIQUE PAR LE PROJET DU SERVEUR S3

J. HERVEG et M.-N. VERHAEGEN [1]

INTRODUCTION

A. – Le développement du traitement informatisé des données du patient dans le secteur des Soins de santé et son écho dans la législation et la réglementation belge

1. Depuis plusieurs années, le secteur des Soins de santé voit apparaître un nombre important d'outils informatiques, combinés le cas échéant avec des moyens de télécommunications. Ces outils participent au traitement automatisé d'informations relatives au patient dans un contexte thérapeutique et ce, à des fins diverses. Ainsi, les praticiens professionnels[2] et les institutions de soins de santé disposent de produits et services pour constituer et gérer le dossier du patient, communiquer et partager diverses données relatives au patient via des réseaux télématiques, faciliter la transmission des données administratives requises en vue de la prise en charge de tout ou partie du coût des soins de santé par l'organisme assureur du patient et par l'assurance maladie-invalidité – sans que cette liste ne soit exhaustive.

1. Centre de Recherches Informatique & Droit, Faculté de Droit de Namur – FUNDP (Belgique). La présente étude ne reflète que l'opinion de ses auteurs. Elle s'appuie sur les travaux réalisés par les auteurs et dont les résultats ont été publiés dans la revue du droit de la santé, 2002-2003/2, p. 56 et s.

2. Tels que définis à l'article 2, 3°, de la loi du 22 août 2002 relative aux droits du patient (*M.B.*, 26 sept. 2002, p. 43.719).

Les administrations de la Santé publique et des Affaires sociales, les organismes assureurs et l'Inami[3] disposent aussi d'applications informatiques et télématiques relatives au traitement des données des patients afin de réaliser leurs missions respectives de contrôle de la qualité des soins de santé, de financement des soins de santé et de contrôle et de maîtrise de leur coût.

De même, certains organismes publics ou privés actifs dans le domaine de la recherche médicale, en ce compris des entreprises pharmaceutiques, créent des bases de données, le cas échéant insérées dans des réseaux télématiques, afin de permettre notamment une meilleure collecte ou diffusion de l'information disponible sur des sujets médicaux précis.

Pour sa part, le patient peut déjà explorer les sites « Santé » disponibles sur le Web[4], communiquer par voie électronique avec son praticien professionnel, sans ignorer, à terme, la possibilité qu'il puisse accéder à ses données par une voie télématique.

A l'arrière plan apparaît aussi le développement de la « télémédecine », soit l'acte médical caractérisé dans sa réalisation par le recours aux moyens de télécommunications, ce qui implique le traitement informatisé des données à caractère personnel du patient.

2. Plusieurs dispositions reflètent en droit belge l'apparition de ces nouveaux outils dans le secteur des soins de santé. Il s'agit principalement des règles relatives au dossier médical et infirmier électronique[5], au dossier médical général (global)[6] et au dossier hospitalier[7].

3. L'Institut national d'assurance maladie-invalidité.

4. La Commission européenne travaille d'ailleurs sur les critères de qualité pouvant être retenus pour les sites « Santé ».

5. Voir : A.R. n° 78 du 10 nov. 1967, relatif à l'exercice des professions des soins de santé, art. 45 bis, à propos des critères et modalités des logiciels de gestion du dossier médical et infirmier électronique.

6. A.R. n° 78, du 10 nov. 1967, *o.c.*, art. 35 duodecies ; A.R. 3 mai 1999 relatif au dossier médical général (aussi connu comme le dossier médical global) ; la loi relative à l'assurance obligatoire soins de santé et indemnités, coordonnée le 14 juillet 1994, art. 36 septies nouveau ; A.R., 14 sept. 1984 établissant la nomenclature des prestations de santé en matière d'assurance obligatoire soins de santé et indemnités, annexe, art. 2, A, (pour les honoraires complémentaires octroyés au médecin de médecine générale qui gère le dossier médical global - prestation 102771). Pour la diminution du ticket modérateur du patient qui confie la gestion de son dossier médical général à son médecin généraliste : A.R., 23 mars 1982 portant fixation de l'intervention personnelle des bénéficiaires ou de l'intervention de l'assurance soins de santé dans les honoraires pour certaines prestations, art. 3. Cette mesure profite à toute la population depuis le 1er mai 2002. Par ailleurs, le conseil national de la promotion de la qualité développe des recommandations pour une bonne utilisation du dossier médical global (A.R., 3 juill. 1996 portant exécution de la loi relative à l'assurance obligatoire soins de santé et indemnités, coordonnée le 14 juillet 1994, art. 122 ter, § 4, 2°). Voir sur le dossier médical général : J. DHONT et Y. POULLET, « Het Algemeen Medisch Dossier : een correcte afweging tussen staatsefficiëntie en de vrijheid van de zorgverlener en de privacy van de patiënt ? », *Rev. dr. santé*, 1999-00, pp. 246-254.

7. L., 7 août 1987 sur les hôpitaux, art. 15, § 1 (dossier médical) et art. 17 quater, § 1 (dossier infirmier) ; A.R., 3 mai 1999 déterminant les conditions générales minimales auxquelles le dossier médical, visé à l'article 15 de la loi sur les hôpitaux, coordonnée le 7 août 1987, doit répondre, art. 1, § 1er.

8. L., 14 juill. 1994, *o.c.*, art. 36 sexies nouveau.

9. Il existe déjà **d'autres identifiants** pour certaines finalités administratives et de sécurité sociale. **Pour les patients** : voir déjà la carte d'identité sociale (A.R., 18 déc. 1996 portant des mesures en vue d'instaurer une carte d'identité sociale à l'usage de tous les assurés sociaux etc. (confirmé par la loi du 26 juin 1997) ; A.R. du 22 févr. 1998 portant des mesures d'exécution de la carte d'identité sociale). **Pour les professionnels des soins de santé** : voir déjà la délivrance d'une carte professionnelle (A.R., du 22 févr. 1998 portant des mesures d'exécution de la carte d'identité sociale).

10. L., 29 janvier 2003 portant création de la banque de données fédérale des professionnels des soins de santé, *M.B.*, 26 févr. 2003.

11. Voir l'avis n° 33/2002 du 22 avril 2002 de la Commission de protection de la vie privée à propos du projet de loi relatif à la création de ce Centre. Dans un premier temps, suite aux critiques du Conseil d'État (Doc. Parl., s.o., 2001-2002, n° 1905/001, pp. 91-96), le Gouvernement fédéral a retiré la partie qui concernait la création de ce Centre du projet de loi « portant des mesures en matière de soins de santé » et qui fut voté à la Chambre le 12 juillet 2002. Le Centre a ensuite été créé par la première loi programme du 24 décembre 2002 (*M.B.*, 31 déc. 2002) (art. 259 et s.).

12. A.M., 15 oct. 2001 fixant les critères d'agrément des médecins spécialistes en gestion de données de santé.

Les médecins se voient par ailleurs accorder une intervention financière par l'assurance obligatoire soins de santé et indemnités, pour l'utilisation de la télématique et pour la gestion électronique des dossiers médicaux. Le Roi doit encore déterminer les conditions et les modalités de celle-ci[8].

Afin d'éviter les risques d'erreurs dans le traitement de données, il est envisagé d'attribuer, dans un contexte de soins de santé, un identifiant spécifique aux patients d'une part et aux praticiens professionnels d'autre part[9]. Le gouvernement fédéral a aussi créé une banque de données fédérale reprenant les coordonnées des professionnels des soins de santé[10]. Il vient de créer le Centre fédéral d'expertise des soins de santé pour se doter d'un instrument moderne d'analyse et d'expertise des informations du secteur des Soins de santé en vue d'une plus grande cohérence entre d'une part l'organisation et la politique des Soins de santé et d'autre part, le financement de ceux-ci[11]. Récemment encore, le Ministre de la Santé publique a arrêté les critères d'agrément des médecins spécialistes en gestion de données santé[12].

Enfin, créé en 1999, la Commission « Normes en matière de Télématique au service du secteur des Soins de Santé » a reçu pour mission de promouvoir l'échange électronique de données dans le secteur des soins de santé, ainsi que l'utilisation de dossiers électroniques axés sur les patients tant en milieu hospitalier qu'ambulatoire[13]. Elle émet à cet effet des avis et des recommandations.

C'est dans ce contexte que plusieurs projets – d'initiative publique ou privée – proposent la mise sur pied de *réseaux télématiques* pour permettre la communication ou le partage de données entre les thérapeutes d'un même patient dans une finalité thérapeutique.

B. – Description du projet pilote du serveur S3

3. Le Ministère belge de la Santé publique soutient plusieurs projets pilotes en ce sens, dont un projet dénommé « Serveur S3 »[14]. L'objectif annoncé est de créer des réseaux télématiques reliant des hôpitaux, des médecins généralistes, des spécialistes, des services médico-techniques, des maisons de repos et de soins, etc. Les praticiens professionnels membres du réseau auraient accès par voie télématique à un répertoire informatisé comprenant les documents disponibles au sein du réseau à propos des patients dont ils ont la charge.

Le développement de ce type de réseau serait justifié par le fait qu'une meilleure circulation de l'information sur le patient – et donc une meilleure communication entre les différents intervenants à la relation thérapeutique – participe à la qualité des soins de santé[15]. En filigrane, il peut aussi s'agir de prévenir des dépenses inutiles en évitant la répétition d'actes déjà réalisés et dont les résultats pourraient être accessibles à l'ensemble des praticiens qui soignent un même patient. Il s'agit assurément d'un intérêt relevant également de la Santé Publique.

13. A.R., 3 mai 1999 portant création d'une Commission « Normes en matière de télématique au service du secteur des soins de santé » (WebSite : http://www.health.fgov.be/telematics/).
14. Le sigle S3 représente les initiales de « Serveur Soins de Santé ».
15. A ce propos, voir : L. DUSSERRE, « La sécurité des échanges électroniques d'informations médicales nominatives entre médecins », in *Le secret professionnel, Aspects légaux et déontologiques. Comparaison avec l'étranger*, Ed. Les Études Hospitalières, 2002, p. 167 et s.

Concrètement, chaque praticien participant au Serveur S3 continuerait à posséder sa propre base de données relatives à ses patients[16]. Un réseau de télécommunication relierait ces différentes bases de données et le serveur conserverait « l'adresse informatique » des documents disponibles à propos de chaque patient. Si un praticien souhaite consulter des informations détenues par un de ses collègues à propos du patient dont il a la charge, il accède à une fenêtre d'application qui reprend la liste des documents disponibles. Le praticien sélectionne alors le document qu'il souhaite consulter. Sa demande doit être fonction de son titre professionnel, de ses compétences et des besoins de sa mission de soins. Le serveur garde la trace de toutes les requêtes d'accès aux documents disponibles et de toutes les opérations informatiques initiées par un utilisateur (cf. *infra* à propos des données accessibles et des pouvoirs des utilisateurs).

4. S'agissant du traitement informatisé des données du patient[17], l'implantation et la mise en œuvre du projet du serveur S3 suscitent un certain nombre de questions principalement au regard de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel[18] (loi vie privée) et au regard des règles relatives au secret médical (art. 458 du Code pénal). D'autres questions surgissent aussi notamment à propos de la responsabilité des utilisateurs du réseau et à propos du dossier du patient. Le présent rapport se limite à examiner certaines de ces questions.

16. Le dossier minimum d'urgence devrait toutefois correspondre à une base de données centralisées sur un serveur « extra-muros », ce qui ne manque pas de poser notamment un problème en terme de légitimité du traitement de données. Un problème supplémentaire pourrait surgir dès lors que la Communauté flamande a instauré un modèle de carte uniforme d'urgence médicale (cf. Décret C. Fl., 23 déc. 1986, portant l'instauration d'une carte uniforme d'urgence médicale et son arrêté d'exécution du 25 juin 1987).
17. Voir : J. HERVEG, M.-N. VERHAEGEN et Y. POULLET, « Les droits du patient face au traitement informatisé de ses données dans une relation thérapeutique : les conditions d'une alliance entre informatique, vie privée et santé », *Rev. dr. santé*, en cours de publication.
18. Telle que modifiée par la loi du 11 décembre 1998 transposant la directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données.

I. – QUELQUES QUESTIONS À RÉSOUDRE AU REGARD DE LA LOI VIE PRIVÉE

A. – La légitimité du traitement des données du patient dans un réseau télématique

1 - Le principe de la légitimité du traitement de données

5. Le patient a droit à ce que ses données à caractère personnel soient collectées pour des finalités déterminées, explicites et légitimes[19]. La loi vie privée pose pour principe à cet égard que le traitement de données à caractère personnel *relatives à la santé* est interdit[20], sauf dans un nombre restreint d'hypothèses fixées par elle[21]. S'agissant de la création d'un réseau télématique visant à faciliter le partage d'informations relatives à des patients à des fins thérapeutiques, la finalité de ce traitement de données trouve *formellement* sa légitimité[22] dans l'hypothèse relative aux finalités thérapeutiques visée à l'article 7, § 2, j, de la loi vie privée[23]. Il faut toutefois encore vérifier *concrètement* la légitimité du traitement en opérant la balance entre les avantages générés par le traitement de données d'une part et les atteintes potentielles et réelles aux droits du patient d'autre part. La question se pose à cet égard de savoir si le consentement du patient, repris d'ailleurs à l'article 7, § 2, a, de la loi vie privée en tant qu'autorisation de traiter des données à caractère personnel relatives à la santé, pourrait pallier au déséquilibre des intérêts en présence et fonder la légitimité du traitement ? *Mutatis mutandis* à propos du secret médical, le consentement du patient ne justifie pas à lui seul et indépendamment de son intérêt, une opération de transfert de données d'un praticien à un tiers, fût-il un autre praticien, même si le consentement du patient a une influence certaine dans la justification d'une divulgation du secret.

Par ailleurs, l'évolution de la notion de soins de santé doit retenir l'attention lors de l'évaluation de la légitimité d'un traitement de données à caractère personnel à des fins thérapeutiques. En effet, l'acte médical paraît de plus en plus remis en cause dans sa logique ponctuelle pour être intégré dans une perspective d'octroi de soins de santé qui transcenderait ses acteurs. Le concept de « *prise en charge globale du patient* » exprime clairement cette évolution. Il s'ensuit un élargissement conséquent du champ d'application de la finalité thérapeutique.

Concrètement, le responsable du traitement est le premier « juge » de la légitimité du traitement. La personne concernée, le patient en l'espèce, pourra contester son jugement, notamment suite à l'exercice de son droit d'accès aux données traitées. La Commission de protection de la vie privée, notamment à l'occasion de l'examen de la déclaration du traitement, pourrait être saisie de la question et émettre un avis ou des recommandations. Un tribunal pourrait aussi connaître de la question suite à une procédure initiée en ce sens par la personne concernée.

2 - L'appréciation de la légitimité du traitement des données du patient dans un réseau télématique

6. Dans l'hypothèse de la constitution d'un réseau télématique en matière de soins de santé, la question se pose de savoir si la taille du réseau ne devrait pas être considérée comme un des critères à retenir pour évaluer sa légitimité, étant entendu que l'extension de l'assise du réseau augmente les risques d'atteinte à la vie privée des patients ? De même, la mise en œuvre d'un identifiant spécifique des patients et des praticiens professionnels ne devrait-elle pas aussi être prise en considération dès lors qu'elle démultiplie le risque d'une interconnexion généralisée des fichiers ?

19. L., 8 déc. 1992, *o.c.*, art. 4, § 1er, 2°. Pour être légitime, le traitement de données ne peut être effectué que dans les cas visés à l'article 5 de la loi du 8 décembre 1992, étant entendu que le simple fait de correspondre à l'un de ces cas n'implique pas *ipso facto* que l'exigence de légitimité soit satisfaite.

20. L., 8 déc. 1992, *o.c.*, art. 7, § 1er.

21. Ces exceptions sont énumérées à l'art. 7, § 2, de la loi du 8 déc. 1992, *o.c.*

22. En sachant que les articles 4, 5, et 7, de la loi du 8 déc. 1992, *o.c.*, s'appliquent cumulativement aux traitements de données à caractère personnel relatives à la santé.

23. L., 8 déc. 1992, *o.c.*, art. 7, § 2, j. : le traitement est autorisé lorsqu'il est nécessaire « *(...) aux fins de médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements soit à la personne concernée, soit à un parent, ou de la gestion de services de santé agissant dans l'intérêt de la personne concernée et les données sont traitées sous la surveillance d'un professionnel des soins de santé* ».

B. – La licéité du traitement des données du patient dans un réseau télématique

7. Le traitement informatisé des données du patient à des fins thérapeutiques doit être licite[24]. A cet effet, il doit satisfaire aux normes légales et réglementaires qui lui sont spécifiques. Par conséquent, outre le respect de la loi vie privée, le traitement de données à des fins thérapeutiques doit aussi respecter les règles particulières du droit médical relatives aux données du patient (par ex. : les règles relatives au secret médical, à la tenue du dossier du patient, à la répartition des fonctions entre les différents praticiens professionnels, à certaines obligations en matière de santé publique, les règles déontologiques). La mise en œuvre d'un réseau télématique suscite diverses interrogations au regard du secret médical (cf. *infra*).

C. – La qualité des données traitées dans un réseau télématique

8. Les données à caractère personnel qui font l'objet d'un traitement au sens de la loi vie privée doivent être exactes et complètes au regard des finalités pour lesquelles elles sont traitées, et si nécessaire, mises à jour[25]. Dans un contexte de soins de santé, l'exactitude et la complétude des données traitées s'apprécie au regard des règles de l'art des praticiens concernés.

Le responsable du traitement doit en tout cas prendre les mesures organisationnelles néeessaires pour que le praticien en charge du patient mette lui-même à jour, efface ou rectifie les données du patient inexactes ou incomplètes, au regard des finalités poursuivies.

La transposition de cette règle est malaisée dans le cadre d'un réseau télématique. En effet, il est difficile d'imaginer, dans le cadre d'un dossier médical « partagé » alimenté et utilisé par plusieurs praticiens, que l'un d'entre eux puisse modifier – sans autre forme de procès – les données encodées par un de ses collègues et qu'il estimerait erronées ou dépassées.

24. Th. LEONARD et Y. POULLET, « La protection des données à caractère personnel en pleine (r)évolution, La loi du 11 décembre 1998 transposant la directive 95/46/C.E. du 24 octobre 1995 », *J.T.*, 1999, p. 385, n° 28.
25. L., 8 déc. 1992, *o.c.*, art. 4, § 1er, 4°, et art. 16, § 2, 1°.

Le principe veut que chaque praticien est et demeure responsable des données qu'il a encodées. Ceci étant, la contestation de la qualité de la donnée encodée par un confrère devrait faire l'objet d'une mesure de publicité dans le réseau. Ensuite, une procédure spécifique devrait être établie pour résoudre ce type de contestation. A cet égard, les praticiens concernés et le patient devraient pouvoir faire valoir leur point de vue. Enfin, le résultat de la contestation devrait apparaître. En cas de correction d'une donnée antérieurement encodée, celle-ci devrait subsister en archivage et le fait de sa correction devrait apparaître aux utilisateurs du réseau.

Enfin, l'exigence du caractère complet des données traitées dans un réseau télématique doit être nuancée au regard du fait que le patient peut s'opposer à tout moment à la « communication » de ses données d'un praticien vers un autre ou vers un tiers (conformément à la théorie du secret partagé) et qu'il peut s'opposer à tout type de traitement de ses données s'il se prévaut de raisons sérieuses et légitimes tenant à sa situation particulière (cf. *infra*).

D. – La limite dans le temps du traitement de données à caractère personnel

9. Au regard de la loi vie privée, les données traitées doivent être « *conservées sous une forme permettant l'identification des personnes concernées pendant une période n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement.* »[26] Plusieurs questions apparaissent à cet égard. D'abord, le patient peut-il exciper du fait que l'autorisation de traiter ses données cesse avec la relation thérapeutique, alors que le médecin a l'obligation de conserver son dossier pendant trente ans au minimum[27] et que la conservation des données durant trente ans se justifie aussi dans la mesure elle s'inscrit dans une finalité autre que celle liée aux soins de santé au sens

26. L., 8 déc. 1992, *o.c.*, art. 4, § 1er, 5°.
27. A.R., 3 mai 1999 déterminant les conditions générales minimales auxquelles le dossier médical, visé à l'article 15 de la loi sur les hôpitaux, coordonnée le 7 août 1987, doit répondre, art. 1, § 3 ; Code de déontologie médicale, art. 46. Voir aussi : S. CALLENS et S. BRILLON, « La conservation du dossier patient », *Rev. dr. santé*, 2001-2002, pp. 176-182. Voyez aussi : *Informatique, libertés et recherche médicale*, Paris, CNRS Ed., 2001, p. 165 et s., n° 412 et s.

strict (par exemple une finalité liée à la mise en cause éventuelle de la responsabilité du médecin)[28] ? Qu'en est-il aussi de la tendance consistant à élargir la notion de finalité thérapeutique non pas à l'acte médical ponctuel mais bien à la prise en charge globale du patient ? Ainsi, dans l'hypothèse d'un dossier médical informatisé « partagé », la durée du traitement pourrait se confondre avec la durée de vie du patient... Par ailleurs, toujours dans le cadre d'un dossier médical informatisé partagé, lorsque le délai de conservation est échu, qui est responsable de la destruction des données ? Le responsable du traitement ? Les praticiens professionnels qui ont soigné le patient et encodé les données (alors qu'ils n'exercent peut-être plus) ? Un « médecin de référence » (choisi par le patient) ne pourrait-il pas remplir adéquatement ces tâches ?

Quant aux demandes de conservation au-delà de son décès formulées par le patient pour assurer une meilleure qualité de soins à ses descendants ou à ses collatéraux, etc., celles-ci ne répondraient-elles pas à une finalité autre qu'à celles liées à ses propres soins ?

E. – Le principe de la collecte des données à caractère personnel relatives à la santé auprès de la personne concernée

10. La loi vie privée énonce le principe selon lequel les données à caractère personnel relatives à la santé doivent être collectées auprès la personne concernée[29]. Dans une relation thérapeutique, la collecte des données auprès du patient paraît aller de soi. Toutefois, de manière subsidiaire, la loi vie privée prévoit que les données relatives à la santé peuvent aussi être collectées auprès d'une autre source à condition que ce soit nécessaire aux fins du traitement de données ou que la personne concernée (ici le patient) ne soit pas en mesure de les fournir[30]. Dans ce cas, la loi vie privée prévoit que le responsable du traitement, ou son représentant, doit, dès l'enregistrement des données ou, si une communication de données à un tiers est envisagée, au plus tard au moment de la première communication des données, fournir à la personne concernée les informations habituelles sur le traitement de données à caractère personnel relatives à la santé. Le responsable du traitement est dispensé de fournir cette information lorsque celle-ci se révèle impossible ou implique des efforts disproportionnés[31] et lorsque l'enregistrement ou la communication des données sont effectués en vue de l'application d'une disposition légale ou réglementaire[32], ce qui n'est pas sans susciter certaines critiques. Dans ces cas, le patient a droit à l'information lors de la première prise de contact, ou, si les données ont été communiquées à un tiers, lors de la première prise de contact entre le tiers et le patient[33]. En effet, dans ces deux cas, l'impossibilité d'informer ne se justifie plus. Le responsable du traitement doit justifier cette impossibilité dans la déclaration faite en exécution de l'article 17, § 1er, de la loi modifiée du 8 décembre 1992[34]. Il faut noter que la Commission publie la liste des responsables du traitement dans le registre public visé à l'article 18 de la loi, avec la mention des motifs justifiant la dispense[35].

11. Dans le cas d'une provenance « externe » d'une donnée, la « transparence » de son origine devrait, selon la *ratio legis* de la loi vie privée, être assurée – que la donnée soit collectée auprès d'un confrère, d'un proche du patient, ou que le praticien dispose d'information sur son patient à raison de soins prodigués à un tiers –. Dans le cadre d'une demande de consultation de données du patient détenues par un autre praticien, la théorie du secret partagé participe à cette transparence puisqu'elle implique que le patient soit informé de cette demande pour pouvoir éventuellement s'y opposer. Ainsi, dans le cas d'un dossier médical partagé, le patient doit être informé des modalités précises de fonctionnement du système impliquant des transferts de données entre les différents thérapeutes qui le soignent. L'on pourrait même inciter les concepteurs de réseaux à prévoir que le patient signe

28. S. CALLENS et S. BRILLON, *o.c.*, p. 176.
29. L., 8 déc. 1992, *o.c.*, art. 1, § 5.
30. L., 8 déc. 1992, *o.c.*, art. 7, § 5. Sur l'appréciation critique de ces dérogations, voir not. : M.-H. BOULANGER, S. CALLENS et S. BRILLON, « La protection des données à caractère personnel relatives à la santé et la loi du 8 décembre 1992 telle que modifiée par la loi du 11 décembre 1998 et complétée par l'arrêté royal du 13 février 2001 », *Rev. dr. santé*, 2000-2001, p. 333.
31. En particulier pour un traitement aux fins statistiques ou de recherche historique ou scientifique ou pour le dépistage motivé par la protection et la promotion de la santé publique.
32. L., 8 déc. 1992, *o.c.*, art. 9, § 2, al. 2.
33. A.R., 13 févr. 2001, *o.c.*, art. 30.
34. A.R., 13 févr. 2001, *o.c.*, art. 31, alinéa 1.
35. A.R., 13 févr. 2001, *o.c.*, art. 31, alinéa 2.

un formulaire de consentement relatif à la mise à disposition de ses données via le réseau. Dans une partie introductive, ce formulaire reprendrait toutes les informations relatives aux modalités de transferts des données entre les utilisateurs.

F. – La sécurité et la confidentialité du traitement des données du patient

12. La sécurité et la confidentialité du traitement des données du patient sont assurées d'une part par des obligations au secret et à la confidentialité, et d'autre part, par des obligations d'adopter des mesures techniques et organisationnelles adéquates principalement destinées à garantir que des personnes « non-autorisées » n'accèdent pas aux données traitées.

1 - Les obligations au secret et à la confidentialité

13. Le professionnel des soins de santé sous la responsabilité duquel est effectué le traitement de données à caractère personnel relatives à la santé, est soumis au secret lors du traitement de données, de même que ses préposés ou mandataires[36]. Cette notion de secret ne se confond pas nécessairement avec le secret professionnel visé à l'article 458 du Code pénal.

Lors du traitement, le responsable du traitement doit veiller à ce que les personnes qui ont accès à ces données soient tenues au respect du caractère confidentiel des données traitées en raison d'une obligation légale, statutaire ou par une disposition contractuelle équivalente[37].

La règle du secret professionnel du praticien professionnel participe aussi à la sécurité du traitement puisqu'il lui fait interdiction, sauf exceptions légales et application de la théorie du secret partagé, de révéler les données couvertes sous peine des sanctions pénales visées à l'article 458 du Code pénal.

36. L., 8 déc. 1992, *o.c.*, art. 7, § 4, al. 3. Voyez les sanctions pénales inscrites au chapitre VIII.
37. A.R., 13 févr. 2001, *o.c.*, art. 25, 3°. Voyez pour le sous-traitant, L., 8 déc. 1992, *o.c.*, art. 16.

2 - Les mesures techniques et organisationnelles destinées à assurer la sécurité du traitement des données du patient

14. La protection de la vie privée et le respect des règles relatives au secret médical requièrent l'adoption de mesures techniques et organisationnelles afin d'assurer la sécurité du traitement des données du patient lors de la simple communication de données par courrier électronique, lors de la constitution et de l'usage d'une base de données informatisées ou d'un réseau télématique dans un contexte de soins de santé.

Le *Conseil de l'Europe*[38] préconise que des mesures appropriées soient prises pour assurer la confidentialité, l'intégrité et l'exactitude des données traitées, ainsi que la protection des patients.

La *loi vie privée* prévoit que le responsable du traitement doit veiller à ce que, pour les personnes agissant sous son autorité, l'accès aux données et les possibilités de traitement soient limités à ce dont ces personnes ont besoin pour l'exercice de leurs fonctions ou à ce qui est nécessaire pour les nécessités du service[39]. Il doit d'ailleurs désigner les catégories de personnes ayant accès aux données à caractère personnel relatives à la santé avec une description précise de leur fonction par rapport au traitement des données visées. Cette liste doit être tenue à la disposiiion de la Commission de la Protection de la Vie privée[40].

Toute personne agissant sous l'autorité du responsable du traitement ou sous celle de son sous-traitant, en ce compris le sous-traitant lui-même, et qui accède aux données, ne peut les traiter que sur instruction du responsable du traitement, sauf exception légale[41].

Le responsable du traitement doit aussi prendre les mesures techniques et organisationnelles requises pour protéger les données contre la destruction accidentelle ou non autorisée, contre la perte accidentelle, ainsi que contre la modification, l'accès et tout autre traitement non autorisé de données à

38. Rec. n° (97) 5, du 13 février 1997, du Comité des Ministres aux États membres, relative à la protection des données médicales, art. 9.2.
39. L., 8 déc. 1992, *o.c.*, art. 16, § 2, 2°.
40. A.R., 13 févr. 2001, *o.c.*, art. 25, 1° et 2°.
41. L., 8 déc. 1992, *o.c.*, art. 16, § 3, sauf exception légale.

caractère personnel. Ces mesures doivent assurer un niveau de protection adéquat compte tenu d'une part de l'état de la technique et des frais qu'entraîne l'application de ces mesures et, d'autre part, de la nature des données à protéger des risques potentiels[42]. Elles devraient faire l'objet d'un examen périodique[43].

Sur avis de la Commission de la protection de la vie, *le Roi* peut adopter des normes appropriées en matière de sécurité informatique pour toutes ou certaines catégories de traitements[44]. A ce jour, aucune norme spécifique n'a été arrêtée. L'imputabilité des données, leur intégrité[45] et leur imputabilité à un praticien[46] constituent autant d'aspects supplémentaires de la sécurité du traitement de données.

Le Conseil national de l'Ordre des Médecins a également rendu plusieurs avis en matière de sécurité de traitements de données à caractère personnel relatives à la santé, dans le cadre d'un contexte thérapeutique[47].

Le Conseil de l'Europe recommande aussi de prévoir une personne indépendante responsable de la sécurité des systèmes d'information et de la protection des données, et compétente pour donner des conseils en la matière.[48] Dans le même ordre d'idées, l'article 17 bis de la loi vie privée prévoit que le Roi peut déterminer que le responsable du traitement désigne un *préposé à la protection des données* chargé d'assurer, d'une manière indépendante, l'application de loi ainsi que ses mesures d'exécution[49].

42. L., 8 déc. 1992, *o.c.*, art. 16, § 4. Voir aussi : Rec. n° R (97) 5, *o.c.*, art. 9.1.
43. Rec. n° R (97) 5, *o.c.*, art. 9.1, al. 3.
44. L., 8 déc. 1992, *o.c.*, art. 16, § 4, al. 3.
45. L'assurance que la donnée n'a pas été altérée ou modifiée.
46. Faut-il prévoir la signature électronique dans certaines hypothèses ? L'arrêté royal du 3 mai 1999, *o.c.*, (art. 2, § 2) prévoit pour la signature d'une série de documents dans le dossier médical hospitalier.
47. Voyez not. les recommandations du Conseil national de l'Ordre des Médecins du 17 février 2001 relatives à la protection de la confidentialité lors de la transmission de données médicales à caractère personnel par le réseau Internet, (chiffrement et signature électronique) et celle du 15 juin 2002 relative à la tenue de bases de données médicales contenant des données nominatives ou identifiables (www.ordomedic.be). Voir aussi les avis suivants : « Séeurité des données transmises par Internet », 20 février 1999 ; « Dossier médical global informatisé », 12 décembre 1998 ; « Dossier médical et infirmier électronique », 17 février 1999 ; « Télématique médicale »; 15 février 1997 ; « Communications électroniques-secret médical », 22 avril 1995.
48. Rec. n° R (97) 5, *o.c.*, art. 9.3.
49. L., 8 déc. 1992, *o.c.*, art. 17 bis.

Cette faculté n'a pas encore été mise en œuvre à ce jour pour les données relatives à la santé dans un contexte de soins de santé.

En tous cas, au sein d'un hôpital, le responsable du traitement doit désigner un *conseiller en sécurité*[50] chargé de la sécurité de l'information (lequel resterait sous l'autorité de l'hôpital). A cet égard, n'aurait-il pas été préférable de désigner une personne « *détachée à la protection des données* » au sens de l'article 17 bis de la loi vie privée[51] ?

Si le responsable du traitement confie le traitement des données à un sous-traitant[52], ce dernier doit apporter des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements. Le responsable du traitement doit veiller au respect de ces mesures notamment par la stipulation de mentions contractuelles. Il doit aussi fixer dans un contrat écrit la responsabilité du sous-traitant à l'égard du responsable du traitement et convenir que le sous-traitant n'agit que sur la seule instruction du responsable du traitement et est tenu aux mêmes obligations que celles auxquelles ce dernier est tenu sur pied de l'article 16, § 3, de la loi vie privée[53].

50. A.R., 23 oct. 1964, *o.c.*, annexe, N 1, annexe A, III, normes d'organisation, 9 quater, g.
51. Sur la distinction des fonctions entre « conseiller en sécurité » et « détaché à la protection des données », même si une personne peut cumuler les deux fonctions, lire l'avis n° 33/2002 du 22 août 2002 de la Commission de protection de la vie privée à propos du Centre fédéral d'expertise des soins de santé : « *(...) le conseiller en sécurité doit effectivement veiller à la sécurité des applications et à la prise des mesures techniques et organisationnelles appropriées de manière à garantir le respect de la confidentialité des données et veiller aux contrôles d'accès et autres. (...) Par ailleurs, la nécessité de veiller lors de chaque traitement au respect d'autres principes de la loi de 1992 comme celui de la proportionnalité, celui de l'accès etc. rend nécessaire l'accomplissement d'une autre fonction : celle de « préposé à la protection des données », notion différente utilisée par la LVP (article 17 bis), notion qui couvre d'autres compétences que celle de veiller à la seule sécurité des données mais comprend également le devoir de « s'assurer de manière indépendante de l'application de la présente loi ainsi que de ses mesures d'exécution », ce qui signifie outre le contrôle du caractère adéquat des mesures de sécurité, celle du contrôle du respect des principes de légitimité, de proportionnalité et du droit d'accès des personnes concernées. La Commission si elle estime fondée la distinction des deux fonctions, ne s'oppose pas cependant pas au fait que ce soit une seule et même personne qui cumule les deux fonctions et joue le rôle de contrôleur interne, étant entendu que la loi garantira à cette personne, l'indépendance indispensable à l'achèvement de cette double tâche et surtout mettra en place la commission sectorielle d'autorisation que la Commission réclame et qui jouera le rôle de contrôleur externe (...)* ».
52. Le sous-traitant est défini à l'art. 1, § 5, de la loi vie privée.
53. L., 8 déc. 1992, *o.c.*, art. 16, §1er.

15. Concrètement, chaque praticien professionnel et chaque institution doivent adopter des règles de sécurité en fonction des caractéristiques propres à leurs activités, sans omettre l'obligation de sensibiliser et de former le personnel.

3 - Quelques applications concrètes des règles relatives à la sécurité et à la confidentialité du traitement des données du patient

16. Divers éléments doivent être retenus lors de l'application des règles relatives à la sécurité et à la confidentialité du traitement des données du patient dans le cadre de la constitution d'une base de données informatiques ou d'un réseau télématique donnant accès à différents praticiens professionnels aux informations disponibles sur leurs patients en support aux soins de santé qu'ils leur prodiguent[54].

Il faut d'abord déterminer les utilisateurs du système et poser les règles de leur identification (mot de passe, empreinte digitale, iris, voix, etc. et usage d'une carte professionnelle). Le moyen d'identification doit être strictement personnel à chaque praticien. Il ne peut donc pas le partager.

Il faut aussi pouvoir s'assurer que le praticien ayant accès aux données est bien en charge du patient (ce qui pourrait impliquer, par exemple dans un réseau télématique, que le lien physique avec le patient soit prouvé par la lecture d'une carte personnelle au patient, sauf cas d'urgence...).

Ensuite, il faut définir les données auxquelles les utilisateurs ont accès. En principe, le praticien ne peut avoir accès qu'aux données néeessaires pour pratiquer son art. En pratique, la gestion de l'accès aux données en fonction de la spécialité et de l'identité du praticien n'est pas évidente. Elle devrait chaque fois susciter un débat éthique et technique au sein des institutions ou réseaux eoneernés. En cas d'urgence, les praticiens ne devraient-ils pas pouvoir accéder sans restriction aux données du patient, dont ils useront en fonction de leurs besoins[55], moyennant un contrôle *a posteriori* renforcé ?

54. Voyez aussi les objectifs de sécurité fixés par la Rec. n° R (97) 5, *o.c.*, art. 9.2.
55. En ce sens, voyez le projet :
PCASSO, http://medicine.ucsd.edu./pcasso/patient/section07.html.

Les pouvoirs de l'utilisateur doivent aussi être définis. Quelle est la durée de son accès aux données ? Peut-il modifier ou supprimer tout ou partie des données ? Peut-il en ajouter ? Peut-il les imprimer ? Faut-il conserver la trace de toutes les modifications apportées aux données ? Que faire pour les médecins à fonctions multiples (médecin-conseil / médecin soignant) ?

D'autres mesures de sécurité doivent encore être envisagées telles que l'installation d'un détecteur de virus, un système de sauvegarde automatique, le dédoublement des bases de données[56], etc.

En cas d'utilisation de l'Internet, des mesures de sécurité doivent être prises pour protéger les données circulant sur le réseau. A cet égard, certaines normes de chiffrement paraissent répondre actuellement de manière satisfaisante à cette exigence (voir à cet égard les recommandations précitées de l'Ordre des médecins).

Un système de traçabilité des accès et des opérations effectuées sur les données du patient doit être implanté pour permettre leur contrôle *a posteriori*. Au préalable, il pourrait être opportun d'adopter des mesures de vérification et de constatation des personnes ou des organismes auxquels des données à caractère personnel peuvent être communiquées par des installations de transmission de données[57].

La loi sur les droits du patient consacre son droit à un dossier conservé en lieu sûr[58], ce qui formalise une obligation certainement préexistante ...

Enfin, dans le cadre d'un réseau télématique dans un contexte de soins de santé, il peut apparaître particulièrement opportun de mettre en place un comité de surveillance. Celui-ci devrait fonctionner de manière indépendante, neutre et interdisciplinaire. Il aurait notamment pour mission de définir les règles de conduite relatives à l'accès aux données par les utilisateurs. Il constituerait aussi un premier contact pour les questions ou les plaintes du patient quant au traitement de ses données.

56. La Rec. n° R (97) 5, *o.c.*, art. 9.2, point i, préconise la constitution de copies de sécurité.
57. En ce sens : Rec. n° R (97) 5, *o.c.*, art. 9.2, point f.
58. Loi relative aux droits du patient, art. 9, § 1.

G. – L'information du patient sur le traitement de ses données

17. Au regard de la loi vie privée, l'information du patient participe à la « *volonté d'assurer à l'individu une transparence des circuits informationnels* (...) »[59]. Elle correspond aussi à une facette de la loyauté du traitement de ses données[60]. Cette information ne se confond pas avec l'information du patient sur son état de santé ou sur les traitements médicaux proposés[61].

1 - L'objet et la qualité de l'information due au patient

18. La détermination de l'objet de l'information à fournir au patient et l'appréciation de sa qualité dépend des objectifs de transparence et loyauté qui lui sont assignés. Il s'en déduit que l'information de la personne concernée doit être *appropriée et adaptée aux circonstances*[62] ou encore, *effective et complète* au regard des circonstances de la collecte des données auprès de la personne concernée[63].

En premier, le patient doit être informé de l'existence du traitement informatisé de ses données à des fins thérapeutiques[64]. Ensuite, le patient doit recevoir les éléments d'information nécessaires pour s'assurer du respect de la loi vie privée et de ses droits[65] et pour pouvoir exercer les droit mis à sa

59. M.-H. BOULANGER, C. DE TERWANGNE et Th. LEONARD, « La protection de la vie privée à l'égard des traitements de données à caractère personnel », *J.T.*, 1993, p. 382, n° 65.
60. Sur l'exigence de loyauté, voyez not. : Th. LEONARD et Y. POULLET, *o.c.*, p. 385, n° 28 ; *Manuel de la vie privée*, Bruxelles, Ed. Politeia, p. 64.
61. Voir la loi relative aux droits du patients, not. les art. 7 et 8.
62. Rec. n° R (97) 5, *o.c.*, art. 5.3.
63. D., 95/46/CE, *o.c.*, considérant 38 ; Rec. n° R (97) 5, *o.c.*, art. 5.3.
64. D. 95/46/CE, *o.c.*, considérant 38 ; Rec. n° R (97) 5, *o.c.*, art. 5.1.a. De manière analogue : Exp. motifs précédant le projet ayant donné lieu à la loi du 8 décembre 1992, Doc. Parl., Ch., *s.o.*, 1990-1991, n° 1601-1, p. 15. Voir aussi : Comm. Pr. Vie privée, avis du 6 août 1993, n° 09/93.
65. L'information due pour le traitement de données à caractère personnel doit porter au moins sur : le nom et l'adresse du responsable du traitement et, le cas échéant, de son représentant ; les finalités poursuivies par le traitement ; les destinataires ou les catégories de destinataires des données ; le caractère obligatoire ou non des réponses ainsi que les conséquences éventuelles d'un défaut de réponse ; l'existence d'un droit d'accès et de rectification de ses données. Ces trois dernières informations (qualifiées de « supplémentaires ») ne doivent pas nécessairement être fournies quand, compte tenu des circonstances particulières dans lesquelles les données sont obtenues, elles ne sont pas nécessaires pour assurer à l'égard du patient un traitement loyal (et transparent) des données (art. 9, § 1er, d, in fine, de la loi du 8 décembre 1992, *o.c.*). Voyez le contenu de l'information définie par l'article 5.1. de la Rec. n° R (97) 5, *o.c.*

disposition à cet effet. Ainsi, par exemple, il doit pouvoir identifier le responsable du traitement, être informé sur la finalité du traitement et sur ses droits d'accès et de rectification, ainsi que, le cas échéant, être informé de son droit d'opposition au traitement.

S'agissant de données à caractère personnel relatives à la santé au sens de la loi vie privée, l'information spécifique[66] à communiquer au patient – ou la déclaration de traitement visée à l'article 17, § 1er, de la loi –, doit mentionner la base légale ou réglementaire autorisant le traitement de données[67].

19. Si le thérapeute entend, dans le même temps, traiter les données non seulement à des fins thérapeutiques mais aussi à des fins de recherche scientifique[68], le responsable du traitement doit au minimum préciser la nature du projet, les objectifs de celui-ci, ainsi que le nom de la personne ou de l'organisme pour le compte duquel est effectuée la recherche[69]. Que ce soit dans le même temps ou ensuite de soins ou dans le cadre d'expérimentations médicales, cette information spécifique rejoint celle qui est due au patient à raison d'atteinte à son intégrité physique[70].

Dans certains cas, le patient a le droit d'obtenir une information spécifique à raison d'une règle juridique particulière. Ainsi, dans la mesure où il doit pouvoir s'opposer *à tout moment* à la communication de ses données d'un praticien à l'autre, le patient doit être préalablement informé de toute communication effective, conformément à la théorie du secret partagé[71].

66. L'information spécifique sur le traitement de données à caractère personnel relatives à la santé s'ajoute à celle déjà due pour le traitement de données à caractère personnel.
67. A.R., 13 février 2001, *o.c.*, art. 25.
68. H. NYS, « Rechtsontwikkelingen inzake de bescherming van de privacy bij de medisch-wetenschappelijk onderzoek », in *Personen en FamilieRecht, Gezin en Recht in een postmodern samenleving*, Gent, Mys & Breesch, pp. 27-54.
69. Rec. n° R (83)10, *o.c.*, art. 3.1. En ce qui concerne les conditions liées au traitement *ultérieur* de données à des fins scientifiques, voir M.-H. BOULANGER, S. CALLENS et St. BRILLON, *o.c.* ; M.-N. VERHAEGEN et J. HERVEG, *o.c.*, p. 128 et s.
70. Voir la Convention sur les droits de l'homme et la biomédecine et son art. 22, la déclaration d'Helsinki de l'association médicale mondiale (mise à jour le 2 oct. 2000) sur les principes éthiques relatifs à la recherche médicale sur les sujets humains, ainsi que la directive 2001/20/CE du 4 avril 2001 concernant le rapprochement des dispositions législatives, réglementaires et administratives des Etats membres relatives à l'application de bonnes pratiques cliniques dans la conduite d'essais cliniques de médicaments à usage humain.
71. M.-N. VERHAEGEN et J. HERVEG, « Quand la « communication » du secret médical à des tiers est mise en cause », in *Le secret professionnel*, Bruxelles, Ed. La Charte, 2002, pp. 109-138.

2 - La manière d'informer le patient sur le traitement de ses données

20. La loi vie privée ne précise pas le mode d'information du patient ; le responsable du traitement ou son représentant doit fournir à la personne concernée les informations visées à l'article 9. En pratique, l'information du patient peut être réalisée par la remise d'un document explicatif ou par un affichage adéquat, sans écarter la possibilité d'une information orale. Néanmoins, le Conseil de l'Europe recommande que chaque personne concernée devrait, de préférence, être informée individuellement[72]. Ceci pourrait permettre de contester l'information du patient par voie collective (ex. par voie d'affichage dans la salle d'attente). En tout état de cause, l'information du patient doit être compréhensible, quitte à recourir à des techniques adéquates de communication.

Dans un hôpital, l'information du patient se réalise en principe par la remise d'office d'un exemplaire du règlement relatif à la protection de la vie privée[73]. Il serait opportun d'envisager une modification réglementaire pour imposer la remise au patient d'un règlement similaire dans les autres types d'offres collectives de soins de santé (maisons de repos et de soins, polyclinique, centres médicaux, etc.), et éviter ainsi le reproche d'une différence de traitement non justifiée.

3 - Le moment de l'information du patient sur le traitement de ses données

21. Le responsable du traitement ou son représentant doit fournir au patient les informations dues au plus tard au moment où les données sont obtenues.

Lorsque les données ne sont pas collectées auprès du patient, son information doit se faire au moment de l'enregistrement des données ou au plus tard lorsque les données sont communiquées pour la première fois à un tiers[74], sauf exceptions[75].

72. Rec. n° R (97) 5, *o.c.*, art. 5.3.
73. A.R., 23 oct. 1964, *o.c.*, annexe, III, Normes d'organisation, 9° quater. Cet arrêté royal n'a cependant pas été mis à jour suite à la modification de la loi du 8 décembre 1992 par la loi du 11 décembre 1998.
74. Sauf lorsque la personne concernée en est déjà informée (L., 8 déc. 1992, *o.c.*, art. 9, § 1er, al. 1. Voir aussi art. 9, § 2, al. 2).
75. D. 95/46/CE, *o.c.*, considérant 39 ; L., 8 déc. 1992, *o.c.*, art. 9, § 2.

Face à un patient inconscient ou en cas d'urgence, l'information devrait pouvoir être postposée jusqu'à ce que le patient soit en état de la recevoir[76]. Entre-temps, l'information doit-elle être communiquée à un proche du patient tel le représentant prévu dans la loi relative aux droits du patient, et qui pourrait, en vertu de celle-ci, demander une consultation du dossier du patient ?

H. – L'accès du patient à ses données

1 - Les différentes règles applicables à l'accès du patient à ses données

22. Controversé dans le milieu médical, l'accès du patient à ses données[77] a fait l'objet de plusieurs réglementations qui n'ont pas toujours été cohérentes. La récente loi sur les droits du patient a pour objectif d'harmoniser ces diverses réglementations. Il apparaît cependant que tous les doutes n'ont pas été effacés.

a) L'accès du patient à son dossier au regard de la loi sur les droits du patient

23. La loi sur les droits du patient habilite le patient à *consulter* lui-même le dossier tenu par le praticien professionnel qui le soigne[78]. Mais le patient n'a jamais accès aux annotations personnelles du praticien professionnel[79],

76. Pour rappel, la loi relative aux droits du patient prévoit l'intervention d'un représentant désigné par le patient pour l'exercice de ses droits. Pourrait-on envisager que l'information se fasse au profit de ce représentant dans la mesure du possible malgré la règle du secret professionnel ? Ne faudrait-il pas en outre répéter l'information auprès du patient qui aurait repris connaissance ?
77. A propos du droit d'accès, voir not. : I. CORBISIER, « Pouvoir et transparence dans la relation thérapeutique », *R.G.A.R.*, 1990, 11.682 ; R.-O. DALCQ, « Consentement et information du patient. Accès au dossier médical », *Rev. dr. santé*, 1997-1998, p.477 ; Th. LOCOGE, « Droits à la consultation du dossier médical », *Rev. dr. santé*, 1997-1998, p.462 ; Y. POULLET, « A propos de la « propriété » du dossier médical, Quelques considérations autour des notions de propriété, droits subjectifs et intérêts », in *Propriété*, Bruges, La Charte, 1996, pp. 301-319 ; D. VAN PEE et M. DUPUIS, « L'accès au dossier médical, l'information du patient et le principe d'autonomie », *Louvain Médical*, vol. 121, n° 7, 7 sept. 2002, pp. 275-281.
78. Loi relative aux droits du patient, art. 9, § 2, al. 1er.
79. La notion d'annotations personnelles a suscité de nombreux commentaires lors des travaux préparatoires. Voir la définition donnée à ce concept dans l'exposé des motifs : Doc. Parl., Ch., *s.o.*, 2001-2001, n° 1642/012, p. 33. La non consultation des annotations personnelles peut se justifier sur base de l'idée de l'intérêt supérieur que représente l'art de soigner par rapport à celui représenté par le droit d'accès. Le professionnel a un document de travail qui lui est réservé. Voir à cet égard J. DHONT et Y. POULLET, *o.c.*, p.251.

pas plus qu'aux données de son dossier qui concernent des tiers[80]. Il est donné suite dans les meilleurs délais à la demande du patient visant à consulter son dossier, et ce, au plus tard dans les quinze jours[81].

S'il le souhaite, le patient peut se faire assister à cette occasion par une personne de confiance désignée par lui, que cette personne soit un praticien professionnel ou non[82].

Le patient peut aussi exercer son droit de consultation par l'entremise de cette même personne de confiance.[83]

Si la personne de confiance est un pratieien professionnel, elle peut consulter également les annotations personnelles contenues dans le dossier du patient[84], mais pas les données du même dossier qui concernent des tiers.

A contrario, la personne de confiance non-praticien professionnel ne peut pas consulter les annotations personnelles ni les données concernant des tiers.

Dans l'hypothèse d'une application de l'exception (du privilège) thérapeutique[85], le patient ne peut exercer son droit de consulter son dossier que par l'intermédiaire d'un praticien professionnel désigné par lui[86]. Ce dernier a aussi accès aux annotations personnelles du praticien professionnel[87], mais pas aux données du dossier qui concernent des tiers.

24. Le patient se voit aussi reconnaître le droit *d'obtenir au prix coûtant une copie* de tout ou partie de son dossier[88]. Le praticien professionnel peut s'opposer à cette demande s'il dispose d'indications claires selon lesquelles le patient subit des pressions afin de communiquer une copie de son dossier à un ou des tiers[89].

80. Loi relative aux droits du patient, art. 9, § 2, al. 3. Ceci implique de prévoir au moins trois catégories de données dans le dossier médical du patient : les donnéea du patient, les données qui concernent des tiers et les annotations personnelles du praticien.
81. Loi relative aux droits du patient, art. 9, § 2, al. 2.
82. Loi relative aux droits du patient, art. 9, § 2, al. 4.
83. Idem.
84. Loi relative aux droits du patient, art. 9, § 2, al. 4.
85. Formellement consacré par l'art. 7, § 4, de la loi relative aux droits du patient.
86. Loi relative aux droits du patient, art. 9, § 2, al 5.
87. Loi relative aux droits du patient, art. 9, § 2, al. 5.
88. Loi relative aux droits du patient, art. 9, § 3, al. 1.
89. Loi relative aux droits du patient, art. 9, § 3, al. 2.

La loi sur les droits du patient crée par ailleurs une fonction de médiation à implanter dans les hôpitaux[90]. Le médiateur pourrait donc éventuellement être saisi d'un litige concernant cette disposition.

b) L'accès du patient à ses données faisant l'objet d'un traitement au sens de la loi vie privée

25. La loi sur les droits du patient a modifié l'article 10, § 2, alinéa 1 et 2, de la loi vie privée relative à la communication des données relatives à la santé à la personne concernée[91], sans porter atteinte à l'article 10, § 1er relatif aux « simples » données à caractère personnel du patient, c'est-à-dire les données non médicales[92].

L'article 10, § 2, al. 1er, de la loi vie privée dispose maintenant que « *Sans préjudice de l'article 9, § 2, de la loi relative aux droits du patient* (article qui concerne la consultation du dossier médical)*, toute personne a le droit, soit directement, soit avec l'aide d'un professionnel des soins de santé, de prendre connaissance des données à caractère personnel traitées en ce qui concerne sa santé* ». Le second alinéa ajoute que « *Sans préjudice de l'article 9, § 2, de la loi relative aux droits du patient, la communication peut être effectuée par l'intermédiaire d'un professionnel des soins de santé choisi par la personne concernée, à la demande du responsable du traitement ou de la personne concernée.* »

26. Le premier enseignement à tirer de cette modification législative est que la consultation du dossier médical du patient faisant l'objet d'un traitement de données au sens de la loi vie privée reste régie par l'article 9, § 2, de la loi sur les droits du patient *(consultation directe ou indirecte)*.[93]

Mais, s'agissant *d'obtenir une copie* de tout ou partie du dossier médical constituant un traitement de données au sens de la loi vie privée, quelle

90. Loi relative aux droits du patient, art. 17.
91. Voir l'article 18 de la loi relative aux droits du patient et l'exposé du motif à ce sujet : http://minsoc.fgov.be/cabinet/2002_02_28_patientrighus.doc.
92. Dont l'application ne sera pas examinée ici.
93. La consultation visée dans la loi relative aux droits du patient équivaut à la prise de connaissance visée à l'article 10, § 2, al. 1, de la loi vie privée, *o.c.*, (Doc. Parl., Ch., *s.o.*, n° 1642/012, p. 31).

disposition appliquer ? L'article 9, § 3, de la loi sur les droits du patient qui habilite ce dernier à obtenir lui-même cette copie ou l'article 10, § 2, alinéa 2, nouveau, de la loi vie privée, qui permet au responsable du traitement d'imposer une communication indirecte des données traitées ? Se pourrait-il que le législateur ait, par mégarde, confondu les paragraphes 2 et 3, de l'article 9 de la loi relative aux droits du patient, dans la nouvelle version de l'article 10, § 2, alinéa 2, de la loi vie privée ? Si oui, l'on pourrait alors considérer que l'article 9 § 3 de la loi relative aux droits du patient (octroi de copie au patient, sauf pression de tiers) reste applicable aux dossiers médicaux faisant l'objet d'un traitement de données au sens de la loi vie privée.

27. Ceci étant, la loi vie privée réserve toujours un régime particulier aux données relatives à la santé traitées *qui ne feraient pas l'objet d'un dossier médical. La prise de connaissance* de ces données par la personne concernée serait directe si celle-ci le demande (sans possibilité, pour le responsable du traitement de s'y opposer) alors que la *communication* des même données pourrait être indirecte si le responsable du traitement le demandait. La pertinence de la distinction entre ces deux dispositions n'apparaît pas de manière évidente, d'autant plus si l'on envisage un accès télématique au profit du patient.

28. D'autres questions surgissent encore. Ainsi, l'article 9, § 2, de la loi sur les droits du patient établit le principe du droit de consultation directe par le patient de son dossier ou avec l'assistance ou par l'entremise d'une personne de confiance. S'agissant des données à caractère personnel traitées en ce qui concerne la santé du patient et qui ne constitueraient pas un dossier médical, la nouvelle mouture de la loi vie privée autoriserait le patient ou le responsable du traitement à solliciter une communication indirecte des données, laquelle devrait alors se faire par l'intermédiaire d'un professionnel des soins de santé et non plus par une « simple » personne de confiance.

Une personne de confiance non professionnel des soins de santé pourrait ainsi assister le patient lors de la consultation directe de son dossier ou exercer ce droit à sa place mais elle ne pourrait pas se voir communiquer les données à caractère personnel traitées en ce qui concerne la santé du patient

si celles-ci ne constituent pas ou ne sont pas reprises un dossier médical, ce qui ne manque évidemment pas de surprendre…

29. Notons que si les données à caractère personnel relatives à la santé du patient sont traitées aux fins de recherches médico-scientifiques, la loi vie privée prévoit que leur communication peut, sous certaines conditions, être différée au plus tard jusqu'à l'achèvement des recherches[94].

c - L'accès du patient à son dossier médical hospitalier au regard de la loi sur les hôpitaux

30. L'arrêté royal du 3 mai 1999 prévoit que « *Le patient ou son représentant légal a le droit de prendre connaissance, par l'intermédiaire d'un médecin choisi par lui, des données du dossier médical qui le concernent* »[95].

Même si elle a clairement fait connaître sa volonté d'établir un droit de consultation directe au profit du patient, la loi sur les droits du patient ne se prononce pas explicitement sur le sort à réserver à cette disposition. Or, à défaut de pareille précision, il n'est pas évident de soutenir que celle-ci serait nécessairement caduque ou supprimée. En effet, l'argument de la spécialité de la législation hospitalière pourrait être mis en avant[96]. Il serait utile que le législateur se prononce rapidement et clairement sur ses intentions en la matière, sachant que l'exposé des motifs de la loi sur les droits du patient insiste sur une harmonisation des dispositions relatives à l'accès (direct) au dossier …

Le dossier infirmier hospitalier, quant à lui, serait d'office soumis à la règle de l'article 9, § 2, de la loi sur les droits du patient (consultation directe ou avec l'assistance ou par l'entremise d'une personne de confiance).

94. L., 8 déc. 1992, *o.c.*, art. 10, § 2, alinéas 3 et 4 : conditions permettant de postposer la communication en cas de recherches médico-scientifiques.
95. A.R., 3 mai 1999, *o.c.*, relatif au dossier médical hospitalier.
96. Sans omettre la question de la compétence de l'État fédéral pour modifier la règle (voir sur la compétence fédérale en matière de soins de santé : Doc. Parl., Ch., *s.o.*, 2001-2002, n°299/3, pp. 59-64). Ne devrait-on d'ailleurs pas étendre la question de la compétence de l'État fédéral à propos de l'adoption de l'arrêté royal du 3 mai 1999 relatif au dossier médical hospitalier ?

2 - Comment concevoir en pratique l'accès du patient à ses données ?

31. La question est double. D'abord, à qui va s'adresser le patient pour consulter son dossier médical ou son droit de prise de connaissance ou de communication des données traitées ? Ensuite, qui est habilité à prendre la décision en réponse à la demande du patient ?

Pour l'accès au dossier médical, le patient doit pouvoir s'adresser au médecin qui a constitué le dossier médical. Celui-ci est certainement habilité à statuer sur sa demande. *Dans un hôpital*, le patient devrait pouvoir s'adresser à un médecin référent qui de même serait habilité à répondre à sa requête d'accès au dossier médical. *Au regard de la loi vie privée* pour les données à caractère personnel traitées en ce qui concerne sa santé, le patient doit pouvoir s'adresser au responsable du traitement. Toutefois, celui-ci n'est pas habilité à statuer. Il doit dès lors répercuter la demande du patient à la personne habilitée pour y répondre, et s'assurer du suivi de la requête.

Dans un réseau, le patient devrait en théorie adresser sa demande de consultation de son dossier ou sa demande de prise de connaissance de ses données traitées, au responsable du traitement qui répercuterait la requête au médecin référent du patient habilité à répondre à la demande de son patient. Cette solution paraît fort pratique, d'autant plus si le médecin référent se confond avec le gestionnaire du dossier médical général (global) du patient, autrement dit, son médecin généraliste.

I. – L'opposition du patient au traitement de données exactes ou inexactes

32. En application de la loi vie privée, le patient a le droit de s'opposer à ce que des données à caractère personnel le concernant fassent l'objet d'un traitement pour des raisons sérieuses et légitimes tenant à sa situation particulière[97].

La théorie du secret médical partagé implique par ailleurs que le patient puisse s'opposer à tout moment à ce qu'une donnée – même exacte ou pertinente –, soit communiquée d'un professionnel des soins de santé à l'autre.

97. L., 8 déc. 1992, *o.c.*, art. 12, § 1er, al. 2.

Dans le cas d'une opposition persistante du patient à la communication d'une donnée le concernant, le professionnel des soins de santé doit informer le patient du risque généré par la non-communication de l'information.

La mise en œuvre de ce droit ne manque pas de poser problème pour assurer la qualité d'un dossier informatisé unique du patient et donc à terme, sa faisabilité. En effet, le dossier du patient pourrait être incomplet sans que tous les utilisateurs intéressés ne le sachent et sans qu'ils ne connaissent l'information manquante. Il pourrait alors paraître moins utile de développer pareil dossier si les praticiens ne peuvent pas être certains de son caractère complet, sauf à revenir sur la volonté d'éviter la répétition d'actes déjà réalisés.

J. – La rectification des données inexactes et la suppression ou l'interdiction de traiter certaines données du patient

1 - La rectification des données traitées à raison de leur inexactitude

33. La loi vie privée autorise le patient à obtenir, sans frais, la rectification de toute donnée à caractère personnel inexacte qui le concerne[98]. La transposition de ce droit aux données à caractère personnel relatives à la santé de la personne concernée est délicate. En effet, quand peut-il être considéré, dans l'exercice de l'art de guérir, qu'une donnée relative à la santé est inexacte ? Est-il utile de distinguer à cet égard entre les données objectives (images médicales, résultats d'analyse, noms, adresses, etc.) et les données subjectives ou non définitives (diagnostics, etc.) ? Cette distinction ne paraît pas décisive dès lors qu'elle ne peut se prévaloir d'aucun argument formel dans le texte de la loi.

Le responsable du traitement ne peut en tout cas pas intervenir directement à propos d'une donnée couverte par le secret médical et encodée par un autre professionnel (cf. supra). Il doit cependant prendre les mesures adéquates pour veiller à la qualité des données traitées[99].

98. L., 8 déc. 1992, *o.c.*, art. 12, § 1er, al. 1er.
99. L., 8 déc. 1992, *o.c.*, art. 4, § 1er, 4°, et art. 16, § 2, 1°.

2 - La suppression et l'interdiction d'utilisation de certaines données

34. Toujours selon la loi vie privée, le patient a le droit d'obtenir, sans frais, la suppression ou l'interdiction d'utilisation de toute donnée à caractère personnel qui le concerne et qui, compte tenu de la finalité du traitement poursuivie, est incomplète ou non pertinente, ou dont l'enregistrement, la communication ou la conservation sont interdits ou encore qui a été conservée au-delà de la période autorisée[100].

3 - Quelques aspects de procédure

35. Pour obtenir la rectification d'une donnée à caractère personnel qu'il considère erronée ou inexacte, le patient adresse une requête en ce sens au responsable du traitement[101]. Celui-ci lui communiquera *in fine* les rectifications éventuellement effectuées (par le professionnel qui a encodé la donnée) en réponse à sa requête. Au préalable, une concertation entre le professionnel qui a encodé la donnée litigieuse et le patient paraît inévitable eu égard à la complexité des données de santé et à leur caractère « non figé »[102]. La fonction de médiation dans les hôpitaux créée par la loi sur les droits du patient pourrait par ailleurs se révéler fort utile à cet égard.

Conformément au droit commun, le tribunal peut ordonner une mesure d'expertise pour procéder à des constatations ou donner un avis d'ordre

100. L., 8 déc. 1992, *o.c.*, art. 12, § 1er, alinéa 5.

101. La procédure est fixée par l'article 33 de l'arrêté royal du 13 février 2001, *o.c.*, qui opère un renvoi à l'article 32 du même arrêté. Dans le mois de la demande, le responsable du traitement doit communiquer les rectifications ou effacements des données à la personne concernée et aux personnes à qui ces données ont été communiquées, pour autant toutefois qu'il ait encore connaissance des destinataires de la communication et que la notification à ces destinataires ne paraisse pas impossible ou n'implique pas des efforts disproportionnés (L., 8 déc. 1992, *o.c.*, art. 12, § 3, alinéa 1).

102. J.P. HEYERICK, « Données personnelles en matière de santé, aspects légaux, éthiques et sociaux du traitement des DPS, par le recours éventuel aux professionnels de la santé et aux nouvelles techniques médicales », http://www.health.fgov.be/EMDMI/fr/dicussion/donnees-pers-sante.htm, p.7 : *En principe, le patient devrait pouvoir avoir la garantie que le médecin ou le travailleur de la santé enregistre et traite ses données d'une manière correcte. Ces données ne pourront être modifiées ou supprimées qu'en concertation étroite entre le patient et le gestionnaire du dossier. De même, l'opportunité de conserver certaines données sensibles peut être évaluée différemment par le médecin et par le patient (consommation de cannabis, tendances sexuelles, ...). Ce type de concertation peut d'ailleurs déboucher sur une plus grande implication du patient dans l'enregistrement des DPS qui le concernent et, partant, une meilleure communication entre le patient et le médecin.... ».*

technique – ce qui ouvre une nouvelle porte à une éventuelle conciliation –. Dès réception de la requête du patient ou dès la notification de l'introduction de l'instance judiciaire jusqu'à une décision coulée en force de chose jugée, le responsable du traitement doit indiquer que les données sont contestées[103].

Suite à l'exercice de ce droit par le patient, peut-on soutenir la possibilité de garder une trace de la correction ou de la suppression de la donnée ? A notre sens, il pourrait être envisagé de conserver le fait de la correction et de la suppression mais, en tout état de cause, la donnée corrigée ou supprimée ne peut pas être conservée en archivage – sauf à méconnaître l'effectivité du droit du patient –.

4 - L'impact des règles relatives au secret médical sur le fonctionnement du réseau télématique dans le secteur des soins de santé

36. Des règles spécifiques au secteur des soins de santé peuvent nuancer les droits à la rectification et à la suppression de certaines données, dans la mesure où les traitements impliquant des « transferts » de données entre professionnels des soins de santé donnent le droit au patient de s'y opposer à tout moment sans avoir d'ailleurs à se justifier et ce, conformément à la théorie du secret partagé. Le patient a dès lors le droit de demander la suppression d'une donnée disponible via le réseau télématique, *même si la donnée est exacte, complète et pertinente*. A cet effet, il pourrait être envisagé que le patient s'adresse au responsable du traitement, lequel répercuterait la demande au professionnel qui a encodé la donnée en vue de la suppression de la donnée en cause (après concertation et dialogue).

La question se pose de savoir si les utilisateurs du réseau doivent être informés de la suppression de pareille donnée et si une trace de la suppression doit être conservée – voire l'archivage de la donnée ? A nouveau, il ne peut être question de remettre en cause l'effectivité du droit du patient à cet égard. Toutefois, ne faut-il pas prendre en considération le risque généré par l'exercice de ce droit qui diminue la qualité de l'information disponible via le réseau ? Ne pourrait-on pas au moins envisager de prévenir les utilisateurs que toutes les données sur le patient ne sont pas disponibles ?

103. L., 8 déc. 1992, *o.c.*, art. 15.

II. – QUELQUES QUESTIONS À RÉSOUDRE AU REGARD DE L'OBLIGATION AU SECRET MÉDICAL

37. Posée en 1973, la question de savoir si un praticien pouvait mettre les données de son patient à disposition de tout autre praticien qui pourrait avoir besoin de les consulter dans le futur grâce à des bases de données informatiques centralisées, avait reçu une réponse négative[104]. Ce problème se pose à nouveau pour certains réseaux télématiques[105]. En effet, au-delà de la mise sur pied d'une messagerie électronique, ceux-ci proposent parfois aux praticiens de rendre accessibles tout ou partie des données de leurs patients à tout collègue consulté ultérieurement par ceux-ci. Cette mise à disposition des données des patients sans autre mesure paraît impliquer autant de dérogations à la théorie du secret partagé : le praticien ignore l'identité du destinataire des données et, ne pouvant pas non plus connaître leur utilisation au moment où il les dépose dans la base de données, il ne peut pas contrôler l'adéquation des informations avec les besoins du destinataire pas plus que sa qualification, ni s'assurer du consentement – informé – du patient à la communication ou au partage de ses données médicales ni de son absence d'opposition à cette communication.

Il pourrait être objecté à cet égard que cette situation ressemble peu ou prou à celle du dossier médical hospitalier du patient. A cet égard, il échet toutefois d'observer d'abord qu'*a priori*, un « réseau » télématique concerne un plus grand nombre de praticiens. Ensuite, ces praticiens ne prodiguent pas nécessairement des soins au sein d'une même structure, alors que cette

104. H. ANRYS, « La protection du secret « déposé » dans un système informatique », *Rev. dr. pén. crim.*, 1973-74, p. 581 et s., spéc. p. 587 et s. : « *Par conséquent, le médecin ne peut déposer une partie de son secret entre les mains d'un tiers, fût-il lui même lié par le secret professionnel, que pour autant que celui-ci soit nanti d'une mission légale envers le malade. Il ne pourrait le faire au profit d'une banque de données centralisant tous les renseignements au profit de quiconque pourrait éventuellement en avoir besoin un jour.*
Ceci implique que les données ne peuvent dans l'état actuel des choses, être confiées à une mémoire centrale que si celle-ci apparaît sous le contrôle exclusif du médecin détenteur originaire du secret, et comme la simple concentration dans l'espace des archives exclusivement personnelles du médecin. (...) »

105. A ce sujet, voir, M.-N. VERHAEGEN et J. HERVEG, « Quand la « communication » du secret médical à des tiers est mise en cause », *o.c.*, pp. 109-138 ; « Le secret professionnel en Belgique », *o.c.*, pp. 191-212.

dernière caractéristique participe grandement à la justification de l'assouplissement des règles du secret médical pour autoriser le partage des données médicales du patient dans un hôpital. En d'autres mots, dans un cas, les destinataires ou les utilisateurs sont internes, connus, et placés sous la responsabilité d'un médecin-chef, tandis que dans l'autre cas, ils sont externes, inconnus et agissent de manière autonome.

Il pourrait aussi être objecté que la constitution d'un dossier patient tenu par l'hôpital sous la responsabilité du médecin en chef ne coïncide pas non plus toujours parfaitement avec les conditions de la théorie du secret partagé[106]. En effet, le dossier médical hospitalier – lorsqu'il est véritablement mis sur pied – ressemble à l'ébauche d'un dossier « centré » sur le patient, et moins à l'idée traditionnelle du dossier médical qui se traduit par une multiplication des dossiers du patient et par leur dispersion entre les mains des divers praticiens consultés. Mais, le dossier hospitalier du patient présente toutefois l'avantage de s'appuyer sur une réglementation spécifique validant sa constitution et son usage[107].

38. Il faut observer que, paradoxalement, la technologie disponible peut permettre de mieux faire respecter les conditions de la théorie du secret partagé dans le cadre d'un réseau télématique tel que le S3, notamment par l'adoption des mesures suivantes :

- en imposant une limite temporelle à la consultation des données du patient,
- en déterminant les données accessibles en fonction des besoins et du profit de l'utilisateur,
- en exigeant qu'un lien « physique » avec le patient soit établi et qui permette de s'assurer que l'utilisateur est bien en charge du patient lors de l'accès à ses données (par ex. par la lecture de la carte SIS du patient),
- en instaurant un contrôle *a posteriori* des accès et opérations réalisées par les utilisateurs, etc.

106. En effet, puisque, par exemple, le médecin qui participe à la constitution du dossier médical ne sait pas non plus toujours qui va le consulter ni dans quel contexte.

107. Ce qui ne devrait pas empêcher les hôpitaux d'élaborer en leur sein des lignes de conduites claires relatives à la question « qui a accès à quoi » au regard de la règle du secret partagé ...

Le contrôle *a posteriori* s'opérerait par le traçage obligatoire des accès demandés et la vérification automatique de la qualité des demandeurs. Ce traçage peut se réaliser facilement par l'enregistrement automatique de l'identification obligatoire du praticien lors de sa demande d'accès (système de log-in). La vérification est aisée dans la mesure où la base de données du serveur d'informations contiendrait un fichier de ces numéros et bloquerait l'accès en cas d'une demande non autorisée[108].

39. Cependant, malgré ces garanties techniques et sachant que le respect des règles relatives au secret médical ne peut être vérifié qu'*a posteriori* et non *a priori*, il semble qu'une disposition légale spécifique devrait habiliter le professionnel des soins de santé, au regard du secret médical, à mettre à disposition les données de son patient pour tout confrère consulté ultérieurement par le biais d'un réseau télématique en-dehors des hypothèses déjà partiellement réglées du dossier médical hospitalier et du dossier médical général.

Le problème du secret partagé dans un réseau télématique se poserait peut-être avec moins d'acuité s'il était envisagé non pas de partager les données mais leurs coordonnées de localisation – obligeant celui qui souhaite y avoir accès à contacter le praticien détenteur des données ainsi localisées.

Concrètement, la mise en œuvre de réseaux télématiques à grande échelle dans le secteur des Soins de santé implique une réflexion fondamentale sur la notion de secret médical. La modification des règles relative au secret médical à envisager sur ce point doit respecter l'article 8 de la Convention européenne des droits de l'homme ; l'ingérence dans la vie privée du citoyen doit être prévue par la loi, être légitime et nécessaire dans une société démocratique.

108. Ce contrôle pourrait être effectué par le patient de manière illimitée dans le temps. Ne pourrait-on pas envisager que ce contrôle soit aussi exercé par tout praticien qui a encodé une donnée ? Celui-ci pourrait, durant une période limitée, vérifier qui a accédé aux données qu'il a lui-même encodées.

III. – QUELQUES QUESTIONS À RÉSOUDRE AU REGARD DE LA RESPONSABILITÉ DES UTILISATEURS

A. – La réparation des dommages du patient sur base de la loi vie privée

40. Indépendamment des règles de droit commun en matière de responsabilité, le patient a le droit de demander réparation au responsable du traitement à raison d'un dommage causé par un acte contraire aux dispositions déterminées par ou en vertu de la loi vie privée[109]. Il profite à cet effet d'un renversement de la charge de la preuve. Ainsi, en cas de dommage avéré, il appartient au responsable du traitement de prouver lui-même que le fait générateur ne lui est pas imputable pour être exonéré de toute responsabilité.

B. – Une responsabilité supplémentaire dans le chef de l'hôpital ?

41. La loi relative aux droits du patient instaure une responsabilité spécifique dans le chef de l'hôpital à raison des manquements commis par les praticiens professionnels qui y travaillent (et apparemment spécialement les médecins indépendants) quant au respect des droits du patient tels que définis dans la loi[110] – donc en ce compris le respect de la vie privée du patient.

L'hôpital ne sera toutefois pas responsable des manquements imputables à des praticiens à l'égard desquels une information préalable destinée au patient en dispose explicitement autrement. Cette information préalable doit concerner les relations juridiques entre l'hôpital et le patient en ce qui concerne les aspects médicaux, infirmiers et d'autres pratiques professionnelles de soins. Elle doit être délivrée à la demande du patient. Cela exclut-il une information d'initiative de l'hôpital à ce sujet ? Une réponse affirmative serait assurément source d'injustice... L'hôpital doit par conséquent être encouragé à développer une information d'initiative dirigée vers sa patientèle.

109. L., 8 déc. 1992, *o.c.*, art. 15 bis.
110. Loi relative aux droits du patient, art. 17, 2°, qui insère un article 17 novies dans la loi sur les hôpitaux.

C. – Évolution de la responsabilité du professionnel des soins de santé à l'égard des données disponibles dans un réseau télématique ?

42. L'évolution du dossier du patient comme un tout même « virtuellement » centralisé (pour un ressort territorial limité), caractérisé par la permanence, alimenté et consulté par tous les différents praticiens soignant le patient, doit aussi retenir l'attention à raison des autres changements qu'il pourrait impliquer notamment en termes de responsabilité. En effet, il pourrait être soutenu que le praticien répond – même si ce n'est pas de manière nécessairement exclusive – des conséquences de l'usage de données encodées par un autre professionnel, et qu'il utilise pour pratiquer son art[111].

Le Conseil national de l'Ordre des Médecins considère d'ailleurs à propos des « *renseignements médicaux jugés utiles, accessibles sur Internet par des médecins inconnus qui seraient amenés à donner des soins urgents aux patients participant au système* » que « (...) *Le médecin qui sera amené à utiliser ces données lorsqu'il dispense ses soins, engage dangereusement sa responsabilité s'il base son attitude thérapeutique sur des données qui n'ont pas été validées. D'où besoin de sécurité, d'authenticité et de confidentialité.* (...) »[112].

Mais, à court ou à moyen terme, le praticien ne sera-t-il pas contraint de donner foi à tout ou partie des informations disponibles via des réseaux télématiques répondant aux exigences légales ? En effet, un des objectifs, qui légitime d'ailleurs aussi l'informatisation du secteur des soins de santé, consiste à éviter la répétition d'actes déjà réalisés – avec la conséquence éventuelle du principe du non-remboursement des actes posés pour vérifier la qualité de l'information déjà encodée –. En outre, la consultation des

111. Voire au titre de son obligation de sécurité relative au matériel utilisé ? Avec le cas échéant un recours en garantie contre le praticien qui aurait encodé la donnée ? (voir sur la notion d'obligation de sécurité : Th. VANSWEEVELT, *De civielrechtelijke aansprakelijkheid van de geneesheren en het ziekenhuis*, *o.c.*, 1997, p. 636 et s., n° 1.005 et s.). *Mutatis mutandis*, on pourrait aussi se référer à cet égard aux recommandations de l'Association médicale mondiale sur les responsabilités et les directives éthiques liées à la pratique de la télémédecine, octobre 1999, 51e assemblée générale, point 13 : ... « *Le médecin qui demande l'avis d'un autre médecin* (dans le cadre de notre étude, cet avis est encodé dans une banque de données) *reste responsable du traitement et du diagnostic qu'il donne au patient ainsi que des décisions le concernant* ».

112. Avis du 15 juin 2002, *B.C.N.*, n° 97, sept. 2002.

informations disponibles via le réseau ne constituera-t-elle pas rapidement une règle de l'art à respecter ? Dans ces conditions, il paraîtrait difficile de soutenir un principe de responsabilité du praticien à raison de la qualité des informations disponibles sur le réseau télématique et qui ne sont pas de son fait – sauf évidemment s'il devait être prouvé que le praticien aurait pu - et donc dû - constater, dans les circonstances de la cause, la mauvaise qualité de l'information utilisée –.
Cette constatation entraînera-t-elle une plus grande prudence dans la communication des données (qui devront faire foi) et risquera-t-elle de rendre les communications plus rares ?

IV. – QUELQUES QUESTIONS À RÉSOUDRE AU REGARD DE LA NOTION DE DOSSIER MÉDICAL / PATIENT

43. La gestion des données du patient oscille actuellement entre deux tendances. *D'une part*, nous avons une conception dans laquelle chaque praticien ouvre un dossier au nom de chaque patient dont il a la charge. Il s'ensuit une multiplicité de dossiers ouverts au nom d'un même patient. Certains praticiens se prétendront d'ailleurs « propriétaire » du dossier médical de leur patient pour en réclamer la gestion exclusive. *D'autre part*, nous avons des projets visant à constituer un dossier informatique « unique », « centralisé » (même si c'est de façon « virtuelle ») et « centré » sur le patient. Certains proposent même d'enregistrer le dossier médical du patient sur un support qui serait conservé par le patient. A chaque consultation, le patient confierait le support au praticien qui pourrait alors consulter et compléter son dossier médical.

Ces deux tendances ne sont pas contradictoires. En effet, il existe assurément une vision équilibrée du dossier médical du patient qui veille à respecter l'équilibre des deux principaux acteurs de la relation thérapeutique : le praticien et le patient. Un réseau télématique qui relie les bases de données personnelles de ses praticiens adhérents paraît répondre à ce souhait s'il implante des mécanismes permettant la mise en œuvre des droits du patient face au traitement informatisé de ses données dont principalement le droit de consulter son dossier médical, d'obtenir la rectification et la suppression ou de s'opposer au traitement de certaines de ses données.

CONCLUSIONS

44. La création de réseaux télématiques dans le secteur des Soins de santé répond à une logique de partage des données du patient entre les différents praticiens amenés à lui prodiguer des soins. Leur création s'inscrit dans l'évolution remarquable de l'objectif assigné à l'acte médical qui se caractérise par le passage d'une intervention ponctuelle individualisée à une prise en charge globale du patient.

L'implantation et l'utilisation du projet du serveur S3 posent différentes questions au regard de la loi vie privée, notamment à propos de la légitimité du traitement de données ainsi généré, de sa licéité au regard des règles relatives au secret médical, de la qualité des données traitées, de la sécurité et de la confidentialité du traitement de données, et des différents droits reconnus au patient à cet égard (droit d'accès, droit d'opposition au traitement de ses données, droit de rectification des données inexactes, etc.).

D'abord, un projet de réseau télématique dans le secteur des soins de santé devrait pouvoir au préalable se prévaloir de l'apport d'une réelle amélioration de la qualité des soins de santé.

Ensuite, un praticien ne devrait participer à pareil réseau télématique que si son obligation au secret médical est respectée. Or, cette mise à disposition de données du patient sans connaître leur destinataire effectif ni ses besoins, ne rencontre pas complètement les conditions actuelles de la théorie du secret partagé. Au-delà des considérations techniques relatives à la sécurité et à la confidentialité du traitement de données, la mise en œuvre du réseau implique une réflexion fondamentale sur le secret médical (« déposé ») et son adaptation éventuelle par voie législative.

Eu égard à la fragilisation de la maîtrise des données par les professionnels, aux risques que les réseaux entraînent en termes de sécurité et à une éventuelle « crainte » des patients quant à leur insertion dans un réseau, l'on ne peut qu'inciter les promoteurs de tels systèmes à prévoir le droit explicite du patient d'obtenir à tout moment une liste des utilisateurs des données avec un relevé des documents que ceux-ci ont consultés (contrôle *a posteriori*). Par ailleurs, il serait judicieux qu'un formulaire de consentement écrit du patient, stipulant ses éventuels souhaits quant aux destinataires des données soit facilement accessible (pourquoi pas sur écran) aux utilisateurs du réseau.

A terme, une réflexion devrait intervenir sur le principe et l'étendue de la responsabilité des utilisateurs du réseau télématique dès lors qu'ils devront se fier à des données qui ne sont pas de leur fait.

La désignation d'un médecin de référence par le patient devrait être considérée dès lors que le réseau donnerait accès à des données encodées par plusieurs praticiens professionnels. Il serait l'interlocuteur du patient pour l'exercice de ses droits d'accès, de rectification, d'opposition, etc.) à l'égard des données relatives à sa santé et qui font l'objet d'un traitement.

Enfin, il ne peut pas être perdu de vue que ces réseaux facilitent grandement l'accès à l'information sur le patient soit par l'accumulation de toutes ses données à un même endroit soit par la création d'un point d'accès qui permet d'accéder via une seule application informatique aux données disponibles sur le patient. Ces réseaux risquent dès lors de susciter rapidement la convoitise et il ne faudra pas attendre longtemps pour que des autorités publiques, les tiers participant au financement du secteur des Soins de santé, les compagnies d'assurances, les employeurs, les firmes pharmaceutiques, etc, demandent et obtiennent l'accès à ces réseaux et aux informations du patient. Le seul consentement libre (?) et informé (?) du patient ne suffit pas à lui seul pour justifier cet accès à des fins non-thérapeutiques.

Il faut en tout cas mettre en garde contre le traitement ultérieur des données relatives à la santé du patient pour des finalités autres que thérapeutiques surtout dans le cadre de ce genre de réseau télématique dans le secteur des soins de santé. En effet, la légitimité et la licéité de ces traitements ultérieurs (notamment au regard des règles relatives au secret médical) ne sont pas acquis. Le principe du caractère exclusif de la finalité thérapeutique du traitement des données relatives à la santé du patient dans ce type de réseau télématique doit, à notre avis, être affirmé et respecté, sauf à s'exposer à terme à des dérives dangereuses pour la confiance de la population dans le système de la santé publique.